TOP SECRET

DF/174-A

ARMY SECURITY AGENCY

115/49/TOPSEC/AS-14

Copy No. 33

CSGAS-14

To:

S-2636

TOP SECRET

DF-174A 115/49/TOPSEC/AS-14

FOUR PAPERS BY FRITZ MENZER

1. The attached is an Army Security Agency translation of four brief papers prepared by Fritz MENZER, former member of and expert on cipher machines for the Army High Command Signal Intelligence Agency (OKH/Gen d NA).

2. These are the first of a series of papers prepared by MENZER at the request of Army Security Agency. MENZER is presently held at the Hq 7707 European Command Intelligence Center; his release is expected approximately 31 January 1950. It is therefore requested that any questions rising from these papers be addressed to AS-14 as soon as practicable, in order that MENZER may be queried on pertinent points.

3. Recipients of this document are referred to TICOM DF-174 for details concerning MENZER's detention and past career.

Translated and Edited: R.W.P.
December 1949

35 copies; 24 pages

Copy No._____

Distribution: Normal

INDEX OF CONTENTS

THE ENIGMA PRINCIPLE

I. General

The Enigma cipher machine was developed about 1925. It is one of the first useful cipher machines to be produced in quantity. As basis of the invention practical use was made of an idea dating from the 15th century. This invention is an alphabetically arranged system of slides consisting of two strips which can be slid one against the other.

Example: Margin: abcdefghijklmnopqrstuvwxyz
Tongue: bcdefghijklmnopqrstuvwxyzabcdef...a

The tongue is movable and is slid one space to the left after the encipherment of a letter. There are therefore 26 different positions. The first plain-text letter is enciphered in the first position, the second plain text letter in the second position, ... and the 26th letter in the 26th position. This is continued until the cycle repeats after the 26th step. This cryptographic system does not satisfy present day security requirements, even if random alphabets are used rather than standard alphabets. This insecurity results from the short period (Frequenz) of 26 steps.

However, if a plain letter is enciphered using, let us say, three slide systems, which bear independently scrambled alphabets, and if encipherment is in three stages, then with careful manipulation security can be increased infinitely. Since there are 26 possible settings for each slide, with three slides $26^3 = 17,576$ different settings can be obtained before there is a repetition. If the drive of the three tongues follows the principle of a counter, then the period is 17,576. When using such a principle, tongue 2 advances one step after 26 steps by tongue 1, tongue 3 advances one step after 26 steps by tongue 2.

In the following example three slide systems are represented in the initial position and in the position after 731 steps taken according to the principle of the counter. To make the process easier to follow, the 26 letters of the plain alphabet in each of these two positions have been transformed into the 26 letters of the cipher alphabet by the aid of slide systems 1, 2 and 3. (See conversion.)

TOP SECRET

EXAMPLE OF A THREE-FOLD SLIDE SYSTEM

EXAMPLE 1 — SLIDE POSITION FOR THE FIRST LETTER

SLIDE 1
MARGIN - E B L D C K U V X A J W I Z R H Y S T O G P Q F N M
TONGUE - B L J T K U A V Y I S C R H Z M Q D X F O P E N G W B L J . . W

SLIDE 2
MARGIN - V C W B U X L Z T A Y D M G S F K N E O H R J P I Q
TONGUE - D U C T R S B N X Y H Z Q A X E W G P V F K M L J O D U C U . . L

SLIDE 3
MARGIN - G P C H O B I W F N A M V E L D Z K U S T J Y R X Q
TONGUE - C M R D Q A N L B K Y I J P N O E G X V W F Z U T S C M . . S

CONVERSION FROM SLIDE 1, 2, 3*
MARGIN - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
TONGUE - F A L N W C J S G T U I R Y P H M K E V Z O X D Q B

EXAMPLE 2 — SLIDE POSITION FOR THE 731ST LETTER

SLIDE 1
MARGIN - E B L D C K U V X A J W I Z R H Y S T O G Q P F N M
TONGUE - B L J T K U A V Y I S C R H Z M Q D X F O P E N G W B L J K U . . T

SLIDE 2
MARGIN - V C W B U X L Z T A Y D M G S F K N E O H R J P I Q
TONGUE - D U C T R S B N I Y H Z Q A X E W G P V F K M L J O D U C T . . U

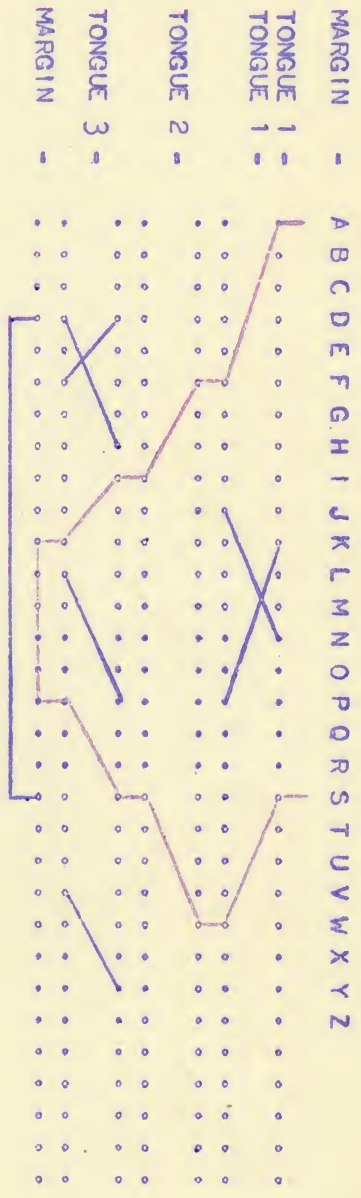
SLIDE 3
MARGIN - G P C H O B I W F N A M V E L D Z K U S T J Y R X Q
TONGUE - C M R D Q A N L B K Y I J P H O E G X V W F Z U T S C M R . . C

CONVERSION FROM SLIDE 1, 2, 3*
MARGIN - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
SLIDE - O R D G Q W P Y S J C N Z L K H D I X A E B U F M V

* ED. NOTE - PLAIN TEXT OVER END IS RESULT OF THE SEVERAL SUBSTITUTIONS

TOP SECRET

EXAMPLE 3


MARGIN -
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
TONGUE 1 -
TONGUE 1 -
TONGUE 2 -
TONGUE 3 -
MARGIN -

Even after careful scrutiny of the cipher alphabets 1 and 731 resulting from these conversions, their causal connection is not recognizable. Therefore the conclusion may be drawn that with the 17,576 different slide positions 17,576 different cipher alphabets can be formed whose sequence is determined by the law governing the drive (counter mechanism principle). In spite of the different structure of the 17,576 cipher alphabets there is, of course, a homogeneous relation among them but this is not to be investigated here. Because of the numerical course of the three slide systems, it is possible to use every position in this period as initial position. The three-fold slide system described above can be simplified in respect to handling if the three tongues have instead of the 52 letters 52 connecting lines in each case and are carried between two margins. For greater clarity only a few connecting lines have been drawn in. Furthermore the letters of the second marginal scale can drop out if in their stead any two letters (positions) are connected with one another by a line. (See Page 2, Example 3.)

The plain-text letter is looked up in margin 1, and the appropriate connecting lines are followed across the three tongues, [along] margin 2, and back across the three tongues to margin 1. After enciphering a letter the three tongues are stepped appropriately. In this way reciprocal relations between the plain-text letters and the cipher letters arise which are advantageous in respect to operation but are disadvantageous with respect to security. (More will be said regarding this later.)

II. Construction of the Enigma

In the construction of the Enigma Cipher Machine the above described reciprocal three-fold slide system has been mechanized. Instead of the three tongues, three rotable cipher wheels A1, 2, 3 have been employed which have 26 electric contacts equally spaced on each face. The contacts of the one face are connected by insulated wires with the contacts of the other face. The marginal scales 1 and 2 have also been developed as wheels. The contact points of the reversing wheel A8 (margin 2) are permanently connected with one another in pairs. The 26 contact points of the entry

wheel A7 are connected with the 26 A-jacks C1 of the plugboard. The 26 B-jacks C2 of the plugboard are connected with the 26 spring contacts of the keys. The A-jacks and B-jacks of the plugboard are put together in pairs and are equipped in each case with a shorting strip (C-3). By the aid of the 2-pole plug connections the shorting connections can be broken and the A-jack of one pair crossed with the B-jack of the other pair. The wheel positions (sequence of the cipher wheels from left to right) and the plug connections are the variable features of the cipher machine. In case a pair of jacks in the plug board is not used the A and B-jacks are connected by the shorting device.

The drive of the three cipher wheels is coupled with the 26 letter-keys D1--26 which simultaneously control the sets of spring contacts E. On one side of each cipher wheel is a ratchet wheel F1 and on the other side a settable ring with a drive notch. The settable ring of one cipher wheel and the ratchet wheel of the adjacent cipher wheel in connection with three stepping ratchets [pawls] F2, which are mechanically connected with the 26 letter-keys, control the movement of the three cipher wheels. The drive of the three cipher wheels works like that of a counter. After 26 steps by the right [sic!] cipher wheel the middle wheel takes one step, after 26 steps by the middle wheel the left [sic!] wheel and the middle wheel take one step together. In this way 26^2 steps are consumed. This function differs from that of the ordinary counting device.

Since this function occurs only every 650 steps while a cipher text must not exceed a maximum length of 180 letters (later of 250 letters), it is not significant.

III. Encipherment

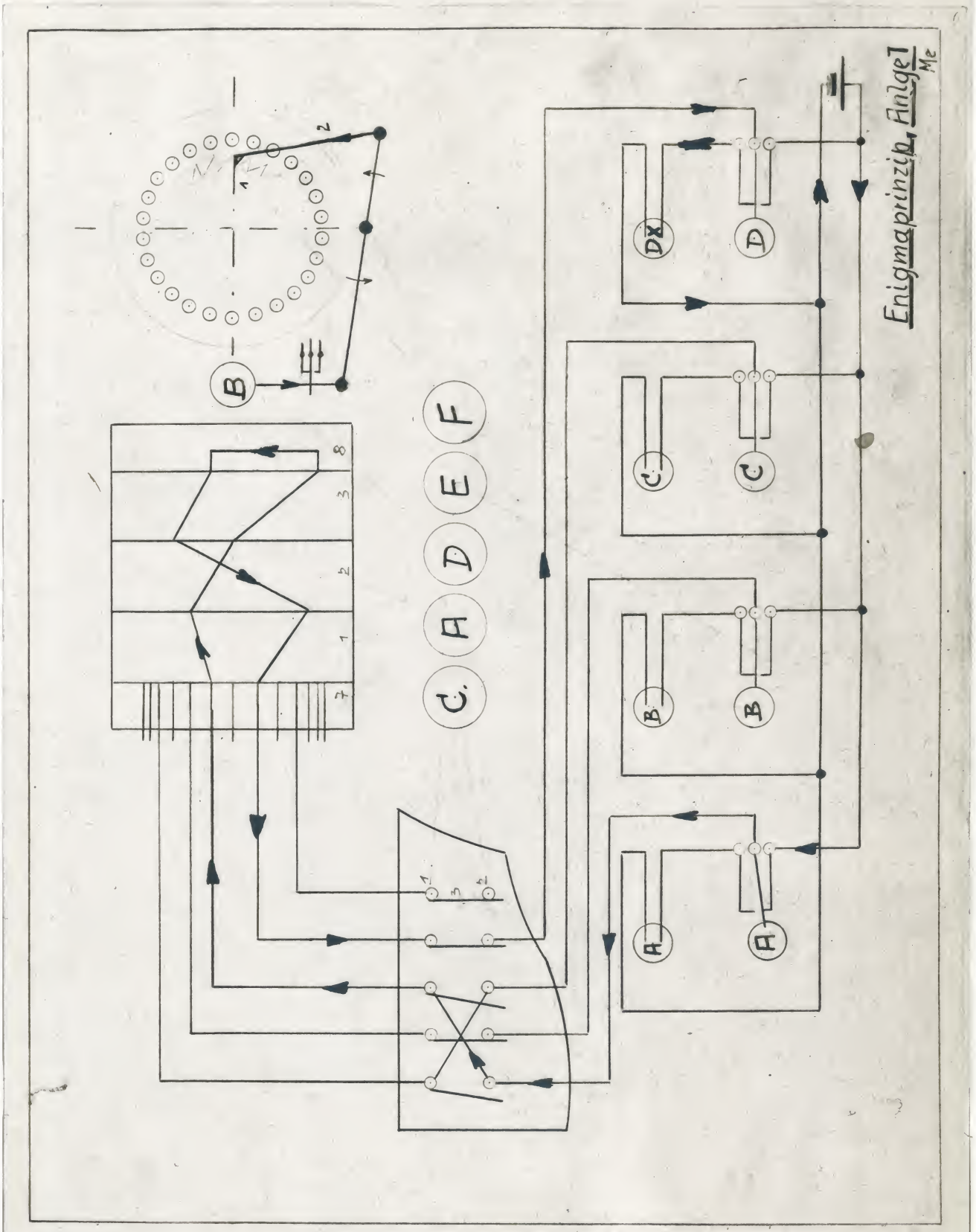
The cipher machine is set up according to a given daily key.

Example: Wheel position: II I V

Ring setting: l v t

Plug connections: gi hb tn cj ms fa lr ek qy dx pw uz

Before enciphering a message key is to be selected in the form of three letters. The three cipher wheels are set to these three letters. Beginning in this position the keys with the corresponding plain-text letters are depressed. The letters illuminated in the lamp field are written down as cipher text. The three letters of the message key are prefixed in enciphered form at the beginning of the cipher text. Decipherment is handled analogously.


Enigmaprinzip, Anlage 1
Me
C A D E F
B
DX
D
C
C
B
B
A
A

CIPHER DEVICE 39
(Precise acquaintance with the Enigma cipher machine is assumed)

I. General

Device 39 is a further development of the Enigma cipher machine in mechanical and crypto-technical respects as well as in regard to operation. It is a completely automatic cipher machine, i. e. by pressing a letter-key the mechanism of the device is set in operation, the corresponding letter (letter on the key board) is enciphered or deciphered and the plain and the cipher letters are printed on separate paper tapes by means of a double type-wheel printer. The cipher text is automatically divided into groups of five letters. Independent of the printing device the cipher letter may also be read off the lamp field.

In this paper only the crypto-technical part is treated.

II. Drive Mechanism[1]

The three pin wheels (Nockenraeder) A 1, 2,3 are mechanically coupled with the three cipher wheels B1,2,3. Mechanical provision is made that the pin wheels A1,2,3 and the cipher wheels B1,2,3 move one step each time a key is pressed. The cipher wheels however are prevented from executing the step, if at the feeler lever C1,2,3 of the associated pin wheel there is a positive pin. The cipher wheels have 26 divisions, pin wheel A1 has 23, pin wheel A2 has 25 and pin wheel A3 has 27. On each pin wheel an odd number (excluding the number 13) of pins is set in the usual way as daily key. The period (Frequenz) of the individual pin wheel corresponds therefore exactly to the number of divisions. That means 23 steps for A1, 25 steps for A2, and 27 steps for A3. The common period of the three pin wheels is the product of the number of divisions 23 x 25 x 27 = 15,525 steps. The period of the cipher wheel is 26 steps when uninfluenced by the pin wheel. The movement of the cipher wheels is dependent however upon the associated pin wheel period. With 23 steps pin wheel A1 makes a full revolution, cipher wheel B1 however makes only 23 steps less the number of positive pins. Since the number of divisions of the pin wheel and the

1. See Supplement.

number of positive pins[2] are prime to 26 (number of divisions of the cipher wheels), we get for A1 - B1 a period of 23 x 26 = 598 steps, for A2 - B2 25 x 26 = 650 steps and for A3 - B3 27 x 26 = 702 steps. Since the position of all three cipher wheels with respect to one another is decisive for the ciphering procedure, the function of the cipher wheels must be considered as a whole. The period of the cipher wheels without the influence of the three pin wheels is 26 steps. Taking into account the 26^3 possible settings and eliminating the cyclic period displacements there are from a crypto-technical point of view 26^2 effectively different basic periods of 26 steps.

Under the influence of the pin wheel functions A - C1,2,3 the basic period of the cipher wheels is lengthened by the product of the number of divisions in the pin wheels A1,2,3. Hence there are 26^2 effectively different periods, whose constant lengths are given by the product of the number of divisions of A1, 2, 3 and B (1,2,3). If the number of divisions A1,2,3 and B1,2,3 are broken up into prime factors, then the product of the different prime factors gives the length of the period and the product of the like prime factors the number of effectively different periods. Hereby the repetitions of prime factors which occur within the number of divisions of one wheel (A2 and A3) must be regarded as different factors because here the unsystematic pin settings (positive and negative position of the pins) is decisive.

	A1	A2	A3	B1	B2	B3
	23	25	27	26	26	26
Prime factors:	23 ·	5·5 ·	3·3·3 ·	2·13 ·	2·13 ·	2·13
Length of the period:	23 · 5·5 · 3·3·3 · 2·13 ..... = 403,676 steps					
Number of periods:	..... 2·13·2·13 = 676 periods					

In the development of Device 39 it was necessary to provide for correspondence with the Enigma when the pins on the pin wheels are put in the negative position.[3] This mechanical function will not be described here because it

2. The difference must be prime. See page 15. [Editor's note]

3. This was demanded by the German Navy. [Editor's note]

represents a purely mechanical demand rather than a crypto-technical necessity. Through this mechanical demand it did come about of course that the 676 periods passed over into one period. In regard to security it appears to be immaterial whether a cipher device yields 676 effectively different periods of 403,676 steps each or one period which is equal to the product of these two factors.

The three cipher wheels are mounted between the entry wheel B7 and the reversing wheel B8. On the sides of the cipher wheels B1-8 are mounted 26 contacts. These contact points are constructed as disk spring contacts. Within each of the cipher wheels B1-8 the 26 contact points on the one side are connected in any desired order with the 26 contact points on the other side. The contact points of the entry wheel B7 are connected to the 26 A-jacks D1 of the plugboard and the 26 contact points of the reversing wheel B8 are connected to a 26 part plugboard E1. These 26 jacks are united in pairs by interchangeable one-pole plug connections E2 (according to key).

With the mechanical rotation of the cipher wheels the contact points necessarily perform a switching function. The 26 A-jacks D1 are united with one another in pairs via the contact points B7, B3, B2, B1,[4] B8, E2, B8, B1, B2, B3, B7. Due to the differing internal circuits of the cipher wheel, which are subject to no particular rule, constantly new combinations result with the 26^3 positions of the cipher wheels.

In contrast to the Enigma two essential advances may be noted in the development of Device 39 in respect to cryptographic technique:

a. The non-uniform and variable stepping of the cipher wheels.

b. The combinations made possible by the variable reversing wheel E1, which moreover is readily changed since it is pluggable.

By these two improvements on the Enigma principle it has become virtually impossible to make Hollerith studies of the constants of the device which would favor the possibility of cryptanalysis.

The following disadvantages, however, are retained which are related to the Enigma principle and which involve an as yet unknown possibility of solution:

---

4. Order of wheels is reversed by error. See Supplement. [Editor's note]

a. The reciprocal structure of the cipher alphabets which is produced by a function of the reversing wheel E1.

b. The two-pole combinations of the plug connections D3, which have a limiting effect on the designations of the keys.

The principle factor of insecurity in all cipher systems remains here, namely, that in spite of all the highly developed mechanical cipher devices, the security of the system is dependent on the choice of the message key. We shall return to this point later.

III. Cipher Process

The cipher process is carried out by means of the 13 circuits which have their beginning and their end in the 26 A-jacks of the plugboard D1, the 26 keys G and lamps F to each of which one letter of the alphabet is associated. The key board and lamp field (type wheel printing system) take over alternately the function of the plain and cipher alphabet. Since the alphabets are reciprocal no change in the wiring is required.

By pressing one of the 26 keys G a set of springs is activated. In so doing two contact springs are opened and two others closed. The one set of contacts H controls the type wheel (represented only by the terminals in Supplement 1). The other circuit, which is controlled by the second set of contact springs, switches in the circuit which makes possible the cipher process by means of the lamp field and the three cipher wheels.

Device 39 is to be set according to the daily key. The daily key consists, for instance, of the following data:

Wheel position: III IV I

Plugboard connections: bh qv do gn ac wy fl tx ei kr pz jn su

Reversing wheel: pn dh io at hs br jq cz fy gx ew lv ku

Pin wheel A1 acegiknprtu (11)

Pin wheel A2 bceghlmprtu (11)

Pin wheel A3 acefhjlmprsuvxz (15)

Before ciphering a text the three cipher wheels and the three pin wheels are to be set in an initial position which hereafter will be called the message key setting. The message key setting is to be treated quite individually because a great part of the security of the cryptogram depends on its selection. (10 messages in phase can be solved, whereby it does not matter which Enigma principle has been employed.)

The 6 letters of the message key are disguised in the usual form and prefixed at the beginning of the cipher text. To agree upon a different position has no significance as far as security is concerned because the letters will be recognized as a kind of indicator group in any case. Beginning with the message key setting, the letters of the plain text are enciphered by pressing the corresponding keys and the appropriate cipher letters are printed by the mechanical printing device. When deciphering the process is analogous.

IV. Choice of the Message Key and Its Consequences

On the basis of the experiences of the last fifteen years an attempt must sometime be made to determine why the analysis of cryptographic systems, some of which were very complicated and diverse, has been successful. Two essential types are noted in this connection:

(1) Cryptanalysis by the aid of compromises of all sorts

(2) Cryptanalysis with the aid of repeated periods (lining up or matching).

The possibilities of cryptanalysis which fall under point (1) can be counteracted in the case of substitution systems by the requirement that reconstruction of the daily key be impossible even with any technical aid. The requirement usually cannot be exactly proven; therefore, here only the most essential studies will be suggested. In this connection, it is naturally assumed that the usual security requirements have been fulfilled.

The possibilities of cryptanalysis which fall under point (2) are per se only special compromises of the cryptographic system. However, this method will be emphasized because it can be employed and can lead to success without any previous knowledge of the cryptographic systems. If, for instance, from a lot of homogeneous traffic single messages are put together which contain more parallel passages or other characteristics than would be expected by the laws of probability, then it may be assumed on the basis of experience that they are in the same key and in the same phase. In the case of the Enigma cryptograms are termed alike in key and phase which were produced by the use of the same daily key and the same setting of the three cipher wheels. In this connection it must be remembered that, due to the cyclic course of the period, only fragments of two cryptograms need be in phase.

Example: 1st cryptogram: dreurntosmnbvcxyasdfghjkl6äü

2nd cryptogram: poiuztrewqasdfghjklmnbvc

If ten cipher texts in phase can be thus lined up, then solution can be accomplished by the aid of column frequencies, etc. Theoretically this possibility of solution is limited by the fact that the relation between the total length of the machine's period and the maximum length of the intercepted messages is so determined that on the basis of probability no repetitions are to be expected. However these considerations are valid only when the appropriate regulations have been observed exactly in the choice of the message key (starting point in the period). The experience of the past fifteen years has shown however that regulations regarding the choice of message keys are quite generally disregarded. The cause is not the evil intent of the responsible person but rather convenience.

Consequently some reflection is in order as to how in the choice of the message key convenience can be furthered and at the same time the entire period exhausted in order to suppress the occurrence of messages in phase. Because experience shows that manual means are inadequate, the solution is to be attained by technical means.

Every cipher device gets a specially developed message key indicator which must at sometime show every message key which can be set up on the cipher device and which is permanently attached to the cipher device. The mechanical course of such a message key indicator must be so constituted that coincidence is ruled out, no matter how many machines are employed. Such a device will be described here, one which fulfills the conditions, is the size of a counter, and is conceived for Device 39 . It may be remarked that the idea is new and has never been put into practical use in crypto-technology.

Six wheels with the divisions 26, 26, 26, 23, 25 and 27 are to be so driven that each wheel takes on the average 13 steps to every 26 drive impulses and collectively yield a period equal to the product of the divisions of the 6 wheels. The drive is by means of a spring which is put under tension when the keys are pressed and can relieve itself of tension

by the unimpeded stepping of the six counter device disks. Using these mechanical principles, the number of steps of the six counter device disks is dependent on the key pressure from each depression of the key to the next and is therefore not subject to control. Each counter disk is inscribed with a random alphabet. In this connection care must be taken that no disk inscription is repeated in any message key indicator among all the cipher devices. By pressing a button the message key indicator can be stopped. The six letters then visible are to be used as message key.

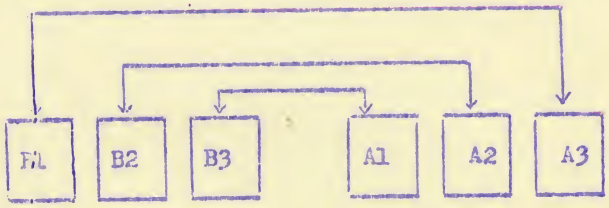
The use of such a message key principle guarantees:

(1) that no message key combination will be repeated for a long time in any one cipher machine,

(2) that the occurrence of cipher texts in the same key and in phase will only be possible by pure chance. Chance, however, can be properly taken care of when constructing a cipher device through the ratio of the period length to the amount of enciphered traffic.

CALCULATION OF THE PERIOD WITH DEVICE 39

1. Drive law :



a. Number of divisions of the pin wheels A1,2,3
A1 = 23, A2 = 25, A3 = 27

b. Number of divisions of the cipher wheels B1,2,3
B1 = 26, B2 = 26, B3 = 26

c. Pin wheels A1,2,3 with their effective pins affect the course of cipher wheels B1,2,3.

d. According to their divisions pins (t) on the pin wheels can be brought into an effective or ineffective position. That pin position is termed effective which checks the course of the cipher wheel.

e. If all pins on pin wheel A1,2,3 are in the ineffective position then pin wheels A1,2,3 and cipher wheels B1,2,3 take one step each time a key is pressed.

f. The number of effective pins is to be determined by the following formula: the number of divisions of the pin wheel less the number of effective pins must be prime to the number of divisions of the cipher wheel.

Number of effective pins = $(tA - n) \not\equiv tB$.

g. The total period is the product of the number of divisions of A1, A2, A3, B1, B2, B3. It breaks up into partial periods if the factors are not prime to one another. The sum of the partial periods is equal to the product of the divisions of all the wheels.

In the present case 26^2 partial periods (B2 x B3) of the length A1 x A2 x A3 x B1 = 23 x 25 x 27 x 26 = 403676 steps are derived.

The following example [in miniature] is intended to illustrate the computation.

Terms: A = pin wheels (t1,2,3)

B = cipher wheels (t4,5,6)

f = steps B4,5,6

t = number of divisions of A1,2,3 or B1,2,3

U = revolutions of A or B

n = number of effective pins on A

F = period

Ziffer = A1,2,3, B4,5,6

h = braking of the course of B4,5,6

A1 = 5, A2 = 7, A3 = 9, B4 = 4, B5 = 4, B6 = 4.

a. Periods without effective pins on the pin wheels:

A1 = 5 steps

A2 = 7 steps

A3 = 9 steps

B4 = 4 steps

B5 = 4 steps

B6 = 4 steps

b. Pin setting (effective pins)

A1) At1 - n ≠ Bt4 = 5 - 2 = 3 ≠ 4 (2 effective pins)

A2) At2 - n ≠ Bt5 = 7 - 4 = 3 ≠ 4 (4 effective pins)

A3) At3 - n ≠ Bt6 = 9 - 6 = 3 ≠ 4 (6 effective pins)

c. Periods: A1B4 = t1 x t4 = 5 x 4 = 20 steps.

A1 12345123451234512345
o o o o o o o o o o effective pins
B4 abbccdaabbccddaabccdd = 20 steps

A2 12345671234567123456712345 67
ooo o ooo o ooo o ooo o effective pins
B5 aaaabbcdddaabccccddabbbbccd = 28 steps

A3 12345678912345678912345678912345 6789
o o oo ooo o oo ooo o oo ooo o oo oo effective pins
B6 aabbccccddddaabbbccccddaaabbbbccdddaa 36 steps

d. Period A1,2,3 = t1 x t2 x t3 = 5 x 7 x 9 = 315 steps

e. Revolutions of a pin wheel during the course of the period of A1,2,3 (315 steps).

$$\frac{F}{At1} = \frac{UA1}{} = \frac{315}{5} = 63UA1, \quad \frac{315}{7} = 45UA2, \quad \frac{315}{9} = 35UA3$$

Hence A1 makes 63 revolutions, A2 makes 45 and A3 makes 35.

f. Number of effective pin functions (brakings of the cipher wheels B4,5,6) within the course of one period of A1,2,3.

A1: h1 = U1 x n1A = 63 x 2 = 126 steps

A2: h2 = U2 x n2A = 45 x 4 = 180 steps

A3: h3 = U3 x n3A = 35 x 6 = 210 steps

g. Number of steps of cipher wheels B4,5,6.

B1: f1 = F-h1 = 315 - 126 = 189 steps

B2: f2 = F-h2 = 315 - 180 = 135 steps

B3: f3 = F-h3 = 315 - 120 = 105 steps

h. Number of revolutions of the cipher wheels within one period of A1,2,3.

B4: $B4U = \frac{f1}{Bt} = \frac{189}{4} =$ 47 1/4 revolutions

B5: $B5U = \frac{f2}{Bt} = \frac{135}{4} =$ 33 3/4 revolutions

B6: $B6U = \frac{f3}{Bt} = \frac{105}{4} =$ 26 1/4 revolutions

1. The period A1,2,3, B4,5,6 is found from the product of the t's.

Nevertheless the period of A1,2,3 B4,5,6 has only run out when all drive wheels and cipher wheels have completed full revolutions at the same time. With 315 steps this is only satisfied for A1,2,3. Wheels B1,2,3 have, as shown in paragraph h, made 1/4, 3/4, and 1/4 too many revolutions. The period A1,2,3 must therefore be run through several times before all six wheels reach the initial position simultaneously.

In running through the periods A1,2,3 the following steps are made.

Full Periods of A1,2,3	Steps	= Cipher Wheel Revolutions		
1	315	B4 47-1/4,	B5 33-3/4,	B6 26-1/4
2	630	B4 94-1/2,	B5 67-1/2,	B6 52-1/2
3	945	B4 141-3/4,	B5 101-1/4,	B6 78-3/4
4	1260	B4 180,	B5 135,	B6 105

The period A1.2.3 B4.5.6 yields, therefore:

F = A1 x A2 x A3 x B4 x B5 x B6 = 5 x 7 x 9 x 4 = 1260 steps

k. In the preceeding example each cipher wheel has 4 positions. With 3 cipher wheels there are therefore 4^3 effectively different positions, that means 4 x 4 x 4 = 64 positions. The pin wheels A1,2,3 have 5 x 7 x 9 = 315 effectively different positions. The runs 1-4 shown in paragraph i had as a result that each of the 315 positions of the pin wheels A1,2,3 came into connection in each case with only 4 of the 64 possibilities of the cipher wheel.

E. g. The position of the pin wheels 1, 1, 1 only occurs in connection with the cipher wheel positions aaa, bcb, cbc, ddd. 4 of the 64 possibilities always occur together so that there are $\frac{64}{4}$ = 16 periods with a lenth of 1260 steps. This number 16 comes from the product B5 x B6 = 4 x 4 = 16. The breaking down of the period given by the product of all 6 wheels into 16 partial periods is the consequence of the equal number of divisions on B4,5,6.

A1 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5

B4 a b b c c d a a b b c d d a a b c c d d a b b c c d a a b b c d d a a

A2 1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7

B5 a a a a b b c d d d d a a b c c c c d d a b b b b c c d a a a a b b c

A3 1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7 8 (23)

B6 a a b b c c c d d d d a a b b b c c c c c d d a a a b b b b c c d d d a

1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5

b c c d d a b b c c d a a b b c d d d a a b c c d d a b b c c d a a b b

1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7

d d d d a a b c c c c d d a b b b b c c d a a a a b b c d d d d a a b

9 1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7 (23)

a a a b b c c c d d d d a a b b b c c c c c d d a a a b b b b c c d d d

1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5

c d d a a b c c d d a b b c c d a a b b c d d a a b c c d d a b b c c

1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7

c c c c d d a b b b b c c d a a a a b b c d d d d a a b c c c c d d a

8 9 1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 (24)

a a a a b b c c c d d d d a a b b b c c c c c d d a a a b b b b c c d d

1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5

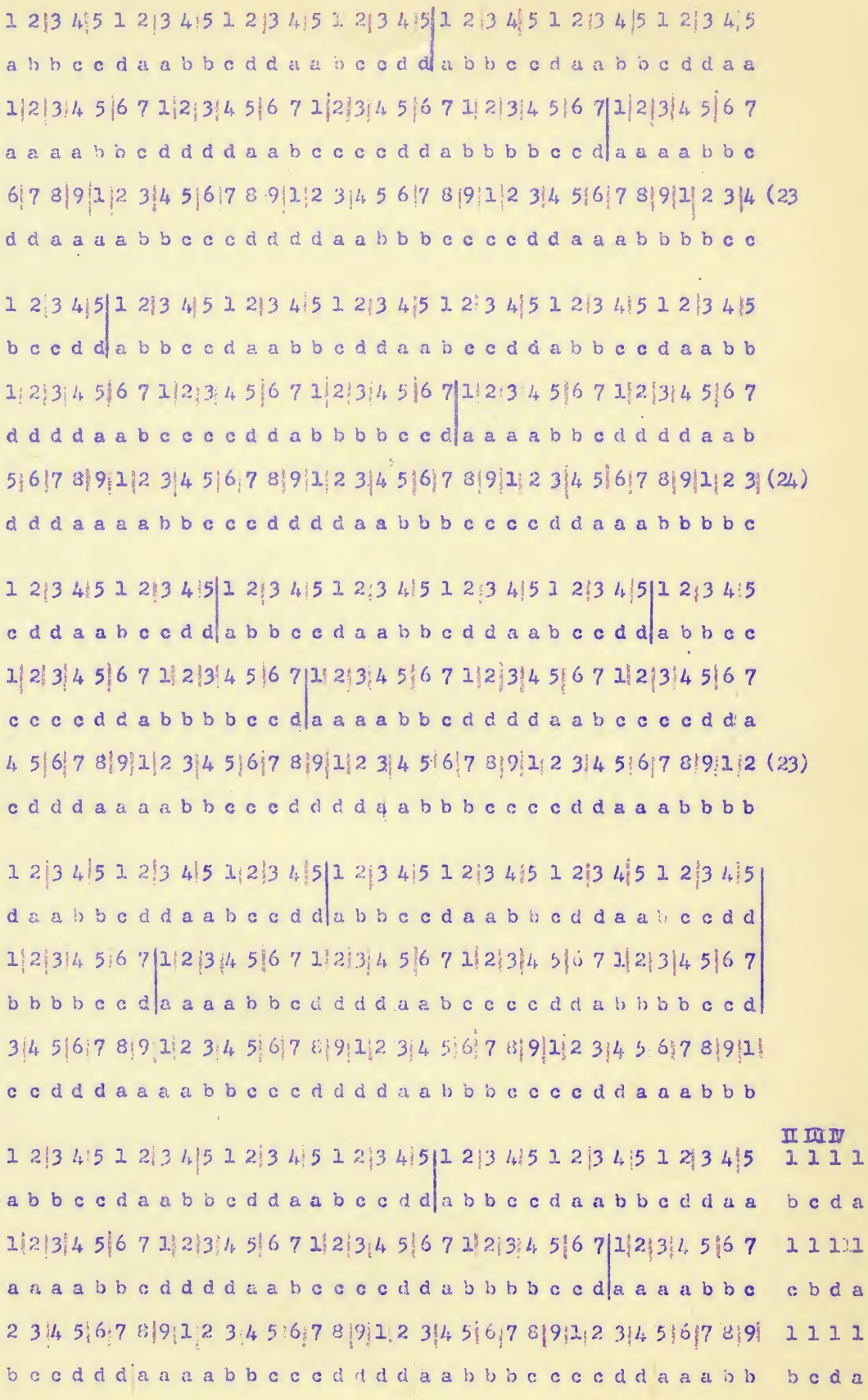
d a a b b c d d a a b c c d d a b b c c d a a b b c d d a a b c c d d

1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7

b b b b c c d a a a a b b c d d d d a a b c c c c d d a b b b b c c d

7 8 9 1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7 8 9 1 2 3 4 5 (23)

d a a a a b b c c c d d d d a a b b b c c c c d d a a a b b b b c c d


(23
(24)
(23)
II III IV

A1 a

	a	b	c	d	A3
a	//	//	///	///	
b	///	///	/	///	
c	//	////	//////	//	
d	////	///	/	///	

A1 b

	a	b	c	d	A3
a	/////	///	/	///	
b	///	///	////	//	
c	//	///	//	////	
d	/	///	////	///	

A1 c

		a	b	c	d	A3
	a	///	//	///	///	
A2	b	////	///	//	//	
A	c	//	////	/////	/	
	d	///	///		////	

A1 d

		a	b	c	d	A3
	a	//////	///	//	///	
A2	b	/	//	///	///	
	c	//	////	///	///	
	d	///	////	////	///	

Run of 180 steps

DIE LUECKENFUELLERWALZE (THE NOTCH FILLER WHEEL)
(Knowledge of the Enigma Principle is Assumed)

The counter-like drive system of the three cipher wheels, the invariable, internal wiring of the wheels, the fixed assignment of the letters to the 26 keys and lamps, and the reciprocal effect of the reversing wheel - which results in the reciprocal structure of the cipher alphabets, have disadvantageous results for the security of the cryptograms.

Due to the fixed internal wiring of the wheels, 17,576 basic cipher alphabets can be derived with each wheel position and their sequence is fixed by the rigid, counter-like drive of the cipher wheels. The variable ring settings on the three wheels have only an insignificant influence on the change of this sequence. (Cyclic displacement.)

The plug connections merely have the effect of a substitution table on the derivation of the basic cipher alphabets, i. e. the characteristics of the cipher alphabets with respect to one another are preserved.

The drive of the three wheels is by three pawls and three ratchet wheels, one associated to each cipher wheel. On the settable rings of the cipher wheels there is in each case one notch. The settable ring of the right wheel[1] in connection with the ratchet wheel of the middle wheel controls the stepping [of the middle wheel] and the ring of the middle wheel in connection with the ratchet wheel of the left wheel controls the stepping [of the latter]. The ring of the left wheel has no effect on the stepping. After 26 steps by the right wheel the middle wheel takes one step, after 26 steps by the middle wheel the left wheel and the middle wheel take one step independent of the function of the right wheel. This function causes the middle and right wheel to have a period of 650 steps instead of 676 possible steps.

---

1. Actually the order is reversed. The left drives the center, and the left and center drive the right. /Editor's note/

The machine constants (wheel wiring, drive notches, etc.) were included as security factors in the assessment of the machine when it was put into use. Assuming a knowledge of the machine, it did not satisfy present day security demands. The reconstruction of the entire daily key was possible by mechanical means provided 15 to 20 letters of enciphered X-text were given. (The letter X had to be enciphered 20 times as plain letter.)

Recognition of this fact led to the development of the Lückenfüllerwalze. Lücke and Antriebskerbe (drive notch) are synonomous. Since the drive notch could be opened in the form of a pin at each of the 26 positions and could be filled again, this cipher wheel was given the name Lückenfullerwalze. Since the construction is carried out only on the settable ring, only the ring with the notch fillers is represented in the supplement. In the case of the Lückenfüllerwalze, however, the ring is rigidly attached to the wheel.

When the Lückenfüllerwalze was put into use it was intended to have three drive notches effective daily in different arrangements. This measure involves a further shortening of the period by some 2000 steps but has a decided influence on the security of the resulting cryptograms.

Moreover other combinations on the Lückenfüllerwalze with respect to the number of effective notches can be employed. In this connection it should be remembered that the number of open notches shall not be a multiple of 2 or 13 and by increasing the number of effective notches the period is correspondingly shortened. It is also possible to subdivide the entire daily key, which in general is valid for 24 hours, by using different arrangements of the notch fillers.

Anlage 1
Lückenfüllerw. Mc 45.1.